



SYSTEMS OF RECORDS NOTICE (SORN) Descriptors

A System of Records (SOR) is a group of records under the control of the National Institutes of Health (NIH) from which a record is retrieved by personal identifier, such as the name of the individual, number, symbol or other unique retriever assigned to the individual. Single records or groups of records which are not retrieved by a personal identifier are not part of a system of records. Records maintained by NIH employees which are prepared, maintained, or discarded at the discretion of the employee are not part of a system of records, unless those records are used to determine rights, benefits, or privileges of individuals in which case, they become agency records subject to the Privacy Act.

09-25-0036 SYSTEMS LISTING

SYSTEM NAME:

Indicates the title of the system of records which accurately describes the records contained within the system.

Extramural Awards and Chartered Advisory Committees (EM-AC 2), Contract Information (DCIS), and Cooperative Agreement Information, HHS/NIH.

SECURITY CLASSIFICATION:

Indicates whether or not the system of records contains classified information.

None.

SYSTEM LOCATION:

Indicates the NIH or contractor office building, room, city and state in which the records system is located, or the server is stored.

Office of Policy for Extramural Research A
Office of the Director (OD), Rockledge II, Room 2172, 6701 Rockledge Drive, Bethesda, MD 20892.

Office of Federal Advisory Committee Policy, Office of the Director (OD), Building 31, Room 3B-59, 31 Center Drive, Bethesda, MD 20892.

Office of Acquisition Management and Policy, Office of the Director (OD), 6100 Executive Boulevard, Room 6D01, Bethesda, MD 20892.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Principal investigators; program and others named in the application (NRSA) trainees and fellows; research advisory committee members; contract personnel; and consultants.

An individual is a living person who is a U.S. citizen or an alien lawfully admitted for permanent residence about whom a record pertains. It does not include persons such as sole proprietorships, partnerships, or corporations. A business firm which is identified by the name of one or more persons is not an individual.

CATEGORIES OF RECORDS IN THE SYSTEM:

Funding applications, awards, historical information pertaining to contracts, and information pertaining to contractors.

The Privacy Act of 1974, as amended (5 U.S.C. 552a) defines a record as “any item, collection, or grouping of information about an individual that is maintained by NIH, including but not limited to the individual’s education, financial transactions, medical history, and criminal or employment history and that contains his name, or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.”

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5. U.S.C. 301; 42 U.S.C. 217a, 241, 282(b)(6), 284a, and 288.

Describes the Government Authorization (Statute or Executive Order) that authorizes the Institute/Center or Office to maintain, collect, use, or disseminate a record and to have control over or responsibility for a system of records.

PURPOSE(S):

1. To support centralized grant programs of the Public Health Service. Services are provided in the areas of grant application assignment and referral, initial review, council review, award processing and monitoring. The database is used to provide complete, accurate, and current information.
2. To maintain communication and coordination of grant activities, including payback obligation through the grant process.
3. To maintain current and historical information pertaining to the establishment or chartered advisory committees of the National Institutes of Health and the appointment or designation of their members.
4. To maintain current and historical information pertaining to contracts awarded by the National Institutes of Health, and performance evaluations on NIH contracts and contracts awarded by other Federal agencies that participate in the NIH Contractor Performance System.

Describes in detail the information that will be collected, maintained, or disseminated and why, and for what purpose the information will be used.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

1. Disclosure may be made to the Department of Commerce for disclosure on funded awards (abstracts and financial data).
2. Disclosure may be made to the subject individual, for a purpose which is compatible with the purpose for which the record was collected. It includes disclosures required to be made by statute other than the Freedom of Information Act (FOIA). It does not include disclosures which are permitted to be made without the consent of the subject individual which are not compatible with the purpose for which it was collected such as disclosures to the Bureau of the Census, the General Accounting Office, or to Congress.
3. Disclosure may be made to a Federal agency, to the extent that the record is necessary for the agency's decision in the matter.
4. Disclosure may be made to a Federal agency upon request for performance information on contractors will be provided to Federal agencies that subscribe to the NIH Contractor Performance System.
5. Disclosure may be made to a Federal agency upon request for performance information on contractors will be provided to Federal agencies that subscribe to the NIH Contractor Performance System.
6. Disclosure of past performance information on contractors will be provided to Federal agencies that subscribe to the NIH Contractor Performance System.
7. A record may be disclosed for a research purpose, when the Department: (A) has determined that the use or disclosure does not violate legal or policy limitations under which the record was provided, collected, or obtained; (B) has determined that the research purpose (1) cannot be reasonably accomplished unless the record is provided in individually identifiable form, and (2) justifies the risk to the privacy of the individual that additional exposure of the record might bring; (C) has required the recipient to (1) establish reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of the record, (2) remove or destroy the information that identifies the individual at the earliest time at which removal or destruction can be accomplished consistent with the purpose of the research project, unless the recipient has presented adequate justification of a research or health nature for retaining that information, and (3) make no further use or disclosure of the record except (a) in emergency circumstances affecting the health or safety of any individual, (b) for use in another research project, under these same conditions, and with written authorization of the Department, (c) for disclosure to a properly identified person for the purpose of an audit related to the research project, if information that would enable research subjects to be identified is removed or destroyed at the earliest opportunity consistent with the purpose of the audit, or (d) when required by law; and (D) has secured a written statement attesting to the recipient's understanding of, and willingness to abide by these provisions.
8. Disclosure may be made to a private contractor or Federal agency for the purpose of collating, analyzing, aggregating or otherwise refining records in this system.

Describes the disclosures that will be made of the information on a routine basis, to whom the information may be released and for what purpose the disclosures will be made. "Routine Use" means the disclosure of a record outside the Department, without the consent of the subject individual, for a purpose which is compatible with the purpose for which the record was collected. It includes disclosures required to be made by statute other than the Freedom of Information Act (FOIA). It does not include disclosures which are permitted to be made without the consent of the subject individual which are not compatible with the purpose for which it was collected such as disclosures to the Bureau of the Census, the General Accounting Office, or to Congress. "Disclosure" means the availability or release of a record to anyone other than the subject individual.

The contractor or Federal agency will be required to maintain Privacy Act safeguards with respect to these records.

9. Disclosure may be made to a grantee or contract institution in connection with performance or administration under the conditions of the particular award or contract.
10. Disclosure may be made to the Department of Justice, or to a court or other adjudicative body, from this system of records when (a) HHS, or any component thereof; or (b) any HHS officer or employee in his or her official capacity; or (c) any HHS officer or employee in his or her individual capacity where the Department of Justice (or HHS, where it is authorized to do so) has agreed to represent the officer or employee; or (d) the United States or any agency thereof where HHS determines that the proceeding is likely to affect HHS or any of its components, is a party to proceed; or (e) HHS determines that the records would help in the effective representation of the individual.

Administrative Safeguards: States policies and procedures that are in place safeguarding the records

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM

STORAGE: Records are stored by name, ID number, and contractor tax ID number.

Describes how the information will be stored (name, ID number, or other personal identifier).

RETRIEVABILITY: Records are retrieved by name, ID number, and contractor tax ID number.

Describes how the information will be retrieved from the records system (name, ID number or other personal identifier).

SAFEGUARDS:

1. Authorized Users: Employees are authorized to grant regular access to records to contract management personnel. Special access by contract management personnel is specifically authorized.
2. Physical Safeguards: Access to work areas is restricted to authorized personnel. Physical access to Office of Acquisition and Policy areas is restricted to OAC personnel. Physical access to OAC files is restricted through IBM password protection. Only authorized personnel are permitted access to OAC files.
3. Procedural Safeguards: Records may be released to staff. Records may be released to manager or other authorized personnel. The use of registered access systems is required.

Describes the administrative, technical and physical/procedural controls in place to minimize the possibility of unauthorized access, use, or dissemination of the information in the record system. Enables authorized use of a record while preventing unauthorized use or use in an unauthorized manner. Ensures methods are in place to ensure least privilege (i.e., "need to know" and accountability) or the necessity for access to, knowledge of, or possession of, specific information required to carry out an official duty. Administrative controls include, but are not limited to user manuals, back-up file storage, privacy awareness training, and contingency plans. Technical controls (user identification, passwords, firewalls, virtual private network, encryption, intrusion detection system, common access cards, smart cards, biometrics and public key infrastructure) are security controls applied to an information system that are primarily implemented by the system through mechanisms contained in the hardware, software, or firmware components of the system. Physical/procedural access controls include, but are not limited to guards, sign in/out logs, identification badges, key cards, cipher locks, biometrics and closed circuit TV.

These practices are in compliance with the standards of Chapter 45-13 of the HHS General Administration Manual, "Safeguarding Records Contained in Systems of Records," supplementary Chapter PHS hf: 45-13, and the HHS Automated Information Systems Security Program Handbook.

RETENTION AND DISPOSAL:

Records are retained and disposed of under the Schedule contained in NIH Manual Chapter "Destroying Records" (HHS Records Management Manual, Appendix B-361), item 4000-A-2, which allows records to be destroyed when no longer needed for administrative purposes. Refer to the NIH Manual Chapter for specific disposition instructions.

Describes the policies or guidelines in place with regard to the retention and destruction of the records and refers to the NIH Records Control Schedule that provides for specific disposition of the records contained within the system.

SYSTEM MANAGER(S) AND ADDRESS:

For Extramural Awards:

Director, Extramural Information Systems, Division of Extramural Research, Office of the Director, Rockledge Drive, Bethesda, MD 20892.

For Chartered Federal Advisory Committees:

Director, Office of Federal Advisory Committee Policy, Office of the Director, Building 31, Room 3B-59, 31 Center Drive, Bethesda, MD 20892.

Lists the responsible NIH official/system manager for a given system of records, or another individual to whom requests may be made, or the designee of either such officer or individual. The notice must include the position title and location of a point of contact for each Institute/Center and Office that manages records. If a point of contact is not listed for a particular IC/Office, it means the organization does not collect, maintain (store), disseminate and/or pass through information in identifiable form (IIF) within any database(s), record(s), file(s) or website(s) that is part of the records system.

For Contracts:

Office of Acquisition Management and Policy, Executive Boulevard, Room 6D01, Bethesda, MD 20892.

NOTIFICATION PROCEDURE:

The requester must also verify his or her identity by providing a written request or a written certification that the requester is who he or she claims to be and understands that the knowing and willful request for acquisition of a record pertaining to an individual under false pretenses is a criminal offense under the Privacy Act, subject to a five thousand dollar fine.

Communicates to an individual whether he is a subject individual about whom a record pertains, and if so, informs him that if he wishes to access records contained within the system, he must certify in writing that he is who he says he is and that if he acquires records under false pretenses, he is subject to criminal penalties under the Privacy Act.

RECORD ACCESS PROCEDURE:

Same as Notification Procedures. Requesters must specify the record contents being sought. Individuals may also request listings of accountable disclosures that have been made of their records, if any.

Informs a subject individual of the availability of a record and asks that they specify the record contents being sought in order to assist NIH in its search for responsive records.

CONTESTING RECORD PROCEDURE:

Contact the official under Notification Procedure to request a copy of the record and specify the information to be corrected, the reasons for the correction, with supporting evidence. The scope of records is limited to information which is incomplete, irrelevant, incorrect, or untimely (obsolete).

Inform a subject individual of the procedure to follow if they wish to correct factual information contained within their record.

RECORD SOURCE CATEGORIES:

Applicant institution, individual, individual's educational institution and references, and participating Federal acquisition personnel.

Inform a subject individual of the original source of the information maintained about them.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

Inform a subject individual if the records system is exempted from disclosure under the Privacy Act of 1974, and if so, lists the exemptions that may be cited.